

REMARKS

35 U.S.C. § 103 rejections: Claims 2-6, 8-14, 16-30, 32-39

Claims 2-6, 8-14, 16-30, and 32-39 have been rejected under 35 U.S.C. § 103 with respect to Vogler (US5815683) in combination with Montague *et al.* (US5675782), Pilc *et al.* (US5510777), and Rosenow *et al.* (US5483596). Four separate references have been required to formulate the rejections in this case. Applicant respectfully asserts that there is no motivation to combine these four references and further asserts that the large number of references needed is an indication that the combination of elements of the present invention is not obvious.

Claim 6 recites:

6. A system on a server computer system, comprising:
 - a communications engine for establishing a communications link with a client;
 - security services coupled to the communications engine for presenting to a user of the client a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it, for authenticating the user according to at least one user authentication protocol and for determining user privileges based on the identity of the user and the level of authentication;
 - a web server for presenting a set of available services based on the user privileges, at least one of the available services requiring additional authentication information to be provided before access to the service is granted, and for enabling the client to select a particular service from the set of available services;
 - a host engine coupled to the security services and to the web server for providing to the client service communication code that enables communication with the particular service; and
 - a key safe for storing keys, each key for enabling communication between the client and a respective service from the set of available services and including all additional authentication information required by the respective service for authenticating the user to the respective service, thereby enabling the client to access the available services without storing the service communication code and keys at the client or having to carry or remember them.

Montague *et al.* disclose software which allows a network administrator to configure access permissions for other users. Montague *et al.* describe the problem by stating that “carrying out routine operations to set or modify access permission to entities on a network that includes multiple servers running multiple operating systems can be both difficult and confusing” [column 5, lines 39-42]. Montague *et al.* disclose an interface which serves to “insulat[e] the user from the various formatting and other operating system-specific access

control parameters” [column 6, lines 9-11] and “translates the request made by the user to the appropriate format from the generic format that was presented to the user” [column 6, lines 60-63].

The software described by Montague *et al.* is a network administration tool, and is not capable of presenting a user a plurality of user authentication protocol options, authenticating the user according to at least one user authentication protocol, and determining user privileges based on the identity of the user and the level of authentication. Thus, at a minimum, Montague *et al.* do not teach “presenting to a user of the client a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it, for authenticating the user according to at least one user authentication protocol and for determining user privileges based on the identity of the user and the level of authentication” as specified in claim 6.

Rosenow *et al.* describe using a matched pair of “access controllers” containing identical sets encryption keys and algorithms [column 17, lines 23-24]. These encryption keys and algorithms are uploaded to the access controllers from a central server “in a very secure manner employing additional measures such as pre-arranged data transfer times” [column 7, lines 60-62] and/or through a “private and dedicated means” [column 8, line 9]. The “access controllers” compare this information in allowing two computers to communicate with each other.

The “access controllers” described by Rosenow *et al.* are required at each and every computer, and do not include a key and all additional authentication information required by a service for authenticating a user. Rosenow *et al.* do not teach using the “access controllers” to enable communication with a set of available services. Thus, at a minimum, Rosenow *et al.* do not teach “a key safe for storing keys, each key for enabling communication between the client and a respective service from the set of available services and including all additional authentication information required by the respective service for authenticating the user to the respective service” as specified in claim 6.

In sum, claim 6 is not rendered obvious by the combination of the four references cited: Vogler, Montague *et al.*, Pilc *et al.* and Rosenow *et al.* No combination of the four references cited teaches each and every element of claim 6. Furthermore, there is no suggestion to combine any of the references.

Claims 20, 29, 30, and 39 include elements that are analogous to claim 6 and are allowable over the cited references for at least the same reasons as given above for claim 6. Claims 2-5 and 8-14 depend from claim 6 and are allowable over the cited references for at least the same reasons. Claims 16-19 and 22-28 depend from claim 20 and are allowable over the cited references for at least the same reasons.

Claim 32 recites:

32. A method, comprising:
receiving, from a client, as an advance communication, security
information corresponding to one or more secured network services;
storing the security information at a location remote from the client;
receiving a user request from a user to access a secured network service;
and
using the stored security information to enable the user access to the
secured network service without requiring the user to supply the stored security
information.

No combination of the four references cited teaches each and every element of claim 32. Furthermore, there is no suggestion to combine any of the references. Claims 37 and 38 include elements that are analogous to claim 32 and are allowable over the cited references for at least the same reasons as given above for claim 32. Claims 33-36 depend from claim 32 and are allowable over the cited references for at least the same reasons.

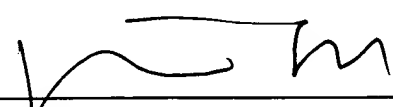
CONCLUSION

Applicants believe that the objections and rejections have been addressed. Applicants respectfully submit that the claims are now in condition for allowance.

Respectfully submitted,

October 21, 2004

Date


Jintung Su
Registration No. 42,174
MANATT, PHELPS & PHILLIPS LLP
1001 Page Mill Road, Building 2
Palo Alto, California 94304
650-812-1375 Telephone
650-213-0286 Facsimile